

## REMARKS

Reconsideration of this application is respectfully requested in view of the foregoing amendment and the following remarks.

Claims 1-31 are pending in this application. In the Office Action, the Examiner objected to the specification and provided guidelines for the revised specification. Claims 11, 14-18 and 29 were objected to for informalities as outlined in the Office Action. Claims 1-5, 8-12, 14 and 29-30 were rejected under 35 U.S.C. § 102(b) as anticipated by Ginter et al. (US Patent Application Publication No. 2002/112171). Claims 1-5, 8-12, 14 and 29-30 were rejected under 35 U.S.C. § 102(b) as anticipated by Cocotis et al. (US Patent Application Publication No. 2002/112162). Claims 6, 7, 13, and 15-27 were rejected under 35 U.S.C. § 103(a) as unpatentable over Ginter et al. (US Patent Application Publication No. 2002/112171). Claims 6, 7, 13, and 15-27 were rejected under 35 U.S.C. §103(a) as unpatentable over Cocotis et al. (US Patent Application Publication No. 2002/112162). Claims 1-11, 14-18, and 29-30 were rejected under 35 U.S.C. §103(a) as unpatentable over Cooper et al. (US Patent No. 7,426,750) and further in view of Mott et al. (US Patent No. 6,170,060). Claims 12-13 and 26-27 were rejected under 35 U.S.C. § 103(a) as unpatentable over Cooper and Mott as applied to claim 1, and further in view of Challener et al. (US Patent Application Publication No. 20030208338). Claims 19-25 were rejected under 35 U.S.C. § 103(a) as unpatentable over Cooper and Mott as applied to claim 1 above, and further in view of Unicte (WO 00/67143). To the extent these rejections might still be applied to claims presently pending in this application, Applicants respectfully traverse the rejections.

### **Amendments to the Specification**

The specification has been amended as requested by the Examiner by adding headings as detailed above. The specification has also been amended to correct certain errors and to maintain consistency throughout the specification. For example, in paragraphs [0050], [0061] and [0062] “decrypt key” now reads “decryption key”; in paragraphs [0094], [0095] and [0112], “digital signs” now reads “digital signatures”; and in paragraphs [0131]-[0135], “authorization table” now reads “authentication table.” The specification has also been amended to recite “U.S. Pat. No.” instead of “U.S. Pat. Application No.” as requested by the Examiner.

### **Claim Objections**

Claims 11, 14, 16, 18 and 29 have been amended to correct certain informalities pointed out by the Examiner. Also, all of the claims have been amended to recite “A method” or “The method” or “A system” or “The system,” instead of “Method” or “System.” Accordingly, the Examiner’s objections to the claims have been overcome.

### **35 USC § 102**

#### The rejection of claims 1-5, 8-12, 14 and 29-30 as anticipated by Ginter

The rejection of these claims as anticipated by Ginter is respectfully traversed. The present invention, as recited in claim 1, is a system and method for performing electronic transactions between a first party and a second party, wherein the first party operates an electronic device such as a personal computer, in which authentication data are stored. Authentication software is provided in the electronic device (e.g., in the personal computer) that can generate a digital signature from the authentication data, which can then be provided to the

second transaction party. As recited in independent claims 1, 9, 29 and 30, the authentication data on the electronic device are inaccessible to the user of the electronic device.

The method and system recited in claims 1, 9, 29 and 30 are not disclosed in Ginter, for at least the reason that Ginter does not disclose a system in which authentication data are inaccessible to the user. To the contrary, Ginter discloses a system in which the decryption key is received by the user. Furthermore, Ginter requires specific hardware for implementing his invention, such as “portable appliances” 600 and 2600 (Ginter, paragraph 1813) and/or requires the use of a “public key” (paragraph 1913). Neither of these is required by the present invention, which indeed explicitly distinguishes systems that use specific hardware (see paragraph [0006] of the application), and does not disclose the use of public keys.

Accordingly, claims 1, 9, 29 and 30, and their dependent claims 2-5, 8, 10-12 and 14 are patentable over Ginter because Ginter does not disclose, teach or suggest a system in which authentication data are inaccessible to the user, and requires specific hardware or the use of a public key. Reconsideration of the rejections in light of the present remarks is earnestly solicited.

Applicants note that the Examiner's general reliance on the international search report, and the search report's cryptic listing of paragraphs [0602], [1302], [1085], [1813], [1913] and Figures 6-8, 35-38, 68-71 and 75 are not in strict compliance with the USPTO's obligations as set forth in MPEP §§ 706 and 707, which requires the Examiner to clearly articulate any rejections, and to do so by designating the particular part of the references that are relevant to the rejections. Specifically, in Ginter, paragraph [0602] is a single short phrase regarding the meaning of “Transparent”; paragraph [1302] describes a process for accessing items stored in a

secure database – which is not particularly relevant to the present invention's generation of a digital signature for authentication purposes; paragraph [1085] simply describes different kinds of content such as software, movies, books, music, etc.; paragraph [1813] describes the use of “portable appliances” which is contrary to the present invention; and paragraph [1913] simply refers to conventional digital signatures using public keys, which is not particularly relevant to the present invention, which relates to generating digital signature, not just using them.

To the extent that the Examiner continues to maintain this rejection, the Examiner is respectfully requested to issue a non-final Office Action, more specifically and clearly explaining the grounds for rejection.

The rejection of claims 1-5, 8-12, 14 and 29-30 as anticipated by Cocotis

The rejection of these claims over Cocotis is respectfully traversed. Cocotis discloses the use of an embedded public key that is transmitted to the user, *i.e.*, the public key is accessible to the user. (See, *e.g.*, Cocotis, paragraphs [0017]-[0019], [0032]-0033] and [0043].) That is contrary to the present invention as recited in claims 1-5, 8-12, 14 and 29-30, which requires the authentication data to be inaccessible to the user. Moreover, the public key is a predetermined key that is independent of the particular transaction, and therefore cannot be considered to be the authentication data of the present invention, which is specific to the transaction. Furthermore, Cocotis fails to disclose or suggest authentication software in the user's electronic device, such that it would be impossible for the Cocotis user to generate a digital signature as required by claims 1-5, 8-12, 14 and 29-30. Accordingly, these claims are patentable over Cocotis, because

Cocotis does not disclose, teach or suggest authentication data that is inaccessible to the user, or authentication software, as recited in claims 1-5, 8-12, 14 and 29-30.

The rejection of claims 1-2, 5-7, 10-11, 28-29 and 31 as anticipated by XTEC

The rejection of claims 1-2, 5-7, 10-11 and 29 as anticipated by XTEC is respectfully traversed. Nowhere does XTEC disclose that its cryptoprocessing key is inaccessible to the user, as required by these claims. *See, e.g.*, page 2, lines 28-34. In fact, at page 3, lines 5-11, XTEC explains that in one embodiment, the hard disk manufacturer's list of defective blocks in a defective block table is used to create the cryptoprocessing keys. Using data supplied by a hard disk manufacturer to generate cryptoprocessing keys is clearly contrary to the present invention as recited in claims 1-2, 5-7, 10-11 and 29, in which the data used to generate the digital signatures are inaccessible to the user.

With respect to claims 28 and 31, XTEC does not disclose an authentication table for generating an encryption key. Instead, XTEC simply discloses that the authentication package or block is encrypted, which is quite different. *See, e.g.*, page 6, lines 22-30 and page 8, lines 7-10. Accordingly, claims 28 and 31 are not anticipated by XTEC.

**35 USC § 103(a)**

Applicants respectfully traverse the rejections of the claims under 35 USC § 103(a) as follows:

- The rejections of claims 6-7, 13 and 15-27 over Ginter and Cocotis are inapposite, because Ginter and Cocotis do not disclose, teach or suggest the invention recited in these claims, as discussed above.

- The rejections of claims 1-11, 14-18 and 29-30 over Cooper in view of Mott are also inapposite because Cooper fails to disclose providing authentication data in a memory of an electronic device that is inaccessible to the user, or authentication software that generates a digital signature, or providing a digital signature to a second transaction party as required by claims 1, 9 and 29. Assuming, *arguendo*, that one of skill in the art would be motivated to combine Mott with Cooper, Mott does not disclose these missing limitations. Instead, Mott discloses a method for matching an ID number embedded in digital form with a device ID or a group ID of a playback device. In fact, the combination of Cooper and Mott would not result in the invention recited in claims 1, 9 and 29, because the Cooper/Mott combination would produce a method in which a player retrieves an ID number from a digital information file; the player ID is compared to the ID contained in the information file; and the information file is played if the IDs match. That is very different from the invention recited in claims 1, 9 and 29, which requires the authentication data to be inaccessible to the user, but accessible to the authentication software and activation of the authentication software to generate a digital signature (claims 1, 9 and 29) that is provided to a second party (claims 1 and 29). Moreover, one of skill in the art would have no reason for looking to Mott to supplement Cooper, because the user of a playback device would have no use for the ID number.
- With respect to claim 30, that claim is patentable over the Cooper/Mott combination, because that combination does not disclose providing authentication data in a memory of an electronic device or digital data having a digital signature embedded therein. Moreover, claim 30 is recited in means-plus-function form, and the Examiner has made

no showing that the structures disclosed in the present application are the same as or equivalent to the structures disclosed in Cooper or Mott.

- Dependent claims 10-11 and 14-18 are patentable over the Cooper/Mott combination because they are dependent upon claim 1, which is patentable as discussed above.
- Dependent claims 12-13 and 26-27 are patentable over the Cooper/Mott/Challener combination because they are dependent upon claim 1, which is patentable as discussed above, and further because the Cooper/Mott/Challener combination does not disclose storing or running authentication data or software that is inaccessible to the operating system of the device. The description in paragraph [0018] of Challener that private keys, digital certificates, etc. reside on two hardware chips is simply not a disclosure that this data is inaccessible to the operating system.
- Dependent claims 19-25 are patentable over the Cooper/Mott/Unicate combination because they are dependent upon claim 1 which is patentable as discussed above. Furthermore, the Cooper/Mott/Unicate combination does not disclose or suggest an authentication table generated from a bit string which is generated from fixed and variable data as recited in claim 20 and its dependent claims 21-24, or an authentication table generated from fixed data, variable data and a bit string, as recited in claim 25. Accordingly, claims 20-25 are patentable for the additional reason that the Mott Unicate combination does not disclose or suggest these additional limitations.

In view of the foregoing, all of the claims in this case are believed to be in condition for allowance. Should the Examiner have any questions or determine that any further action is

desirable to place this application in even better condition for issue, the Examiner is encouraged to telephone Applicants' undersigned representative at the number listed below.

PAUL, HASTINGS, JANOFSKY & WALKER LLP  
875 15th Street, N.W.  
Washington, D.C. 20005  
Tel: 202/551-1847

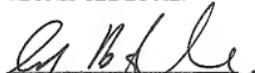
Respectfully submitted,

TEUNIS TEL ET AL.

Date:

November 30, 2009

By:

  
Aslan Baghdadji  
Registration No. 34,542

AB/hjm

Customer No. 36183